GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exemptions and Exceptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State.

MA-1 POLICY AND PROCEDURES

This document addresses the requirements set forth by the State to implement the family of Maintenance security controls at the organization, process and/or system level for all information assets and State data.

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls in this policy based on the National Institute of Standards and Technology (NIST) SP 800-53r5 Security and Privacy Controls.

The “MA” designator identified in each section represents the NIST-specified identifier for the Maintenance control family. The following subsections in this document outline the Maintenance requirements that each agency must implement and maintain to be compliant with this policy. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an Executive Branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

To maintain the highest level of system availability and protect the agency’s infrastructure, maintenance operations must be performed at predetermined, authorized times or on an approved, as-needed basis.

Maintenance policies and procedures developed and maintained to facilitate implementation of information system security maintenance requirements and controls must be reviewed and updated at least every three (3) years or when State-defined changes occur.

MA-2 CONTROLLED MAINTENANCE

Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes:

a. Date and time of the maintenance;
b. Name of individuals or group performing the maintenance;
c. Name of escort, if necessary;
d. A description of the maintenance performed or to be performed; and
e. System components or equipment removed or replaced (including identification numbers).

To accomplish this, the State shall:

a. Establish normal change controls and maintenance cycles for resources managed by OIT;
b. Perform maintenance of those resources in accordance with approved information technology security requirements;
c. Consider the following issues when supporting operating systems:
    i. Update operating system configurations to mitigate newly identified security risks and vulnerabilities;
    ii. Perform periodic maintenance such as hard drive defragment to improve and/or maintain operating system performance; and
    iii. The operating systems on servers, minicomputers, and mainframes usually require daily maintenance tasks and routines that may be initiated manually due to an alert or logged event or may be scripted to run automatically when a certain threshold or limit is exceeded.
d. Ensure system administrators apply all current maintenance and security vulnerability patches and only essential application services and ports are enabled and open in system and network firewalls;
e. Maintain logs of system and system component maintenance and conduct reviews on a regular schedule, comparing the maintenance logs to other system logs to ensure the following:
    i. Maintenance tasks continue to function as expected;
    ii. Operating systems are operating within accepted thresholds;
    iii. System security is not compromised by maintenance tasks; and
    iv. Maintenance tasks do not adversely affect computer capacity or performance.
f. Ensure software faults or bugs are formally recorded and reported to those responsible for software support and maintenance;
g. Restrict physical access to systems;
h. Apply a comprehensive set of management tools to update with approved change management and patch management processes;
i. Monitor information systems so events such as hardware failure and attacks can be detected and responded to effectively;
j. Review maintenance records on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed on the server or other equipment;
k. Provide or arrange maintenance support for all equipment that is owned, leased, or licensed by the agency;
l. Arrange support services through appropriate maintenance agreements or with qualified technical support staff;
m. When maintenance support is provided by a third party, non-disclosure agreements (NDAs) shall be signed by authorized representatives of the third party before any maintenance support is performed;

n. Schedule, perform, document, and review records of information system security maintenance, repairs, and replacement on information system components as required by manufacturer or vendor specifications and organizational requirements;
o. Maintain records of all maintenance activities;
p. Approve and monitor all maintenance activities to include routine scheduled information system security maintenance and repairs, whether the system or system component is serviced onsite or remotely;
q. Ensure removal of the information system or any of its components from the facility for maintenance, repair, or replacement is first approved by an appropriate official;
r. Sanitize equipment to remove all sensitive or confidential information from associated media, following proper procedures when the information system or any of its components require offsite information system security maintenance, repairs, or replacement;
s. Verify proper functionality of all potentially impacted security controls after information system security maintenance or replacement is performed; and
t. Restrict the use of root/administrator privilege to the minimal access required for duties.

MA-3 MAINTENANCE TOOLS

The State shall approve, control, and monitor the use of information system security maintenance tools and maintain these tools on an ongoing basis, and compare previously approved system security maintenance tools as required.

MA-3 (1) MAINTENANCE TOOLS – INSPECT TOOLS

Inspect all maintenance tools carried into a facility by information system security personnel for unauthorized modifications or malicious code. If an incident results from inspection, it shall be handled consistent with State incident response policies and procedures.

MA-3 (2) MAINTENANCE TOOLS – INSPECT MEDIA

Check all media containing diagnostic and test programs for malicious code before introduction into the information system.

If inspected media contains maintenance diagnostic and test programs, incident handling shall be consistent with the State's incident handling policies and procedures.

MA-3 (3) MAINTENANCE TOOLS – PREVENT UNAUTHORIZED REMOVAL

Prevent the unauthorized removal of maintenance equipment which can include, but is not limited to, hardware/software diagnostic test equipment and hardware/software packet sniffers, as follows:

a. Verify that there is no State or agency data contained on the equipment;
b. Sanitize or destroy the equipment; and
c. Retain the equipment within the facility, release it to the Alabama Department of Economic and Community Affairs (ADECA), or a third-party disposal facility upon management approval explicitly authorizing the removal of the equipment.

MA-4 NONLOCAL MAINTENANCE

Nonlocal (remote access) maintenance and diagnostic activities of information systems is allowed only as consistent with State policy and documented in the security plan for the information system and shall be conducted by individuals through either internal or external networks with the following requirements:

a. Approve and monitor nonlocal maintenance and diagnostic activities;
b. Employ multi-factor authentication (MFA) that combines at least two mutually independent factors such as challenge / response answers, biometrics, and tokens for nonlocal maintenance and diagnostic sessions to protect the integrity and confidentiality of communications;
c. Maintain records for nonlocal maintenance and diagnostic activities; and
d. Terminate session and network connections when nonlocal maintenance is completed.

MA-5 MAINTENANCE PERSONNEL

All individuals performing hardware or software maintenance on State or information systems shall have the proper access authorizations to connect to networks to perform maintenance activities.

a. Establish a process for information system security maintenance personnel authorization and maintain a current list of authorized information system security maintenance organizations or personnel;
b. Verify that non-escorted personnel performing information system security maintenance have appropriate access authorizations to the information system allowing access to State data; and
c. Designate personnel with required access authorizations and technical competence to supervise the information system security maintenance activities of personnel who do not possess the required access authorizations.

MA-6 TIMELY MAINTENANCE

Preventative information system security maintenance support shall be performed for the purpose of maintaining equipment and facilities in satisfactory operating conditions.

a. Predictive maintenance or condition-based maintenance shall be performed by conducting periodic or continuous (online) equipment condition monitoring; and
b. Where technically configurable, automated mechanisms should be used to transfer predictive maintenance data to a computerized maintenance management system.

Support for Operating Systems

Operating systems used to run production environments shall be regularly monitored for security risks and maintained in approved secure configurations to support business operations. The following issues should be considered when supporting operating systems:

a. New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities;
b. The operating systems of on-premises hardware such as servers usually require daily maintenance tasks and routines that may be initiated manually as a result of an alert or logged event or may be scripted to run automatically when a certain threshold or limit is exceeded; and

c. Logs of operating system maintenance should be regularly reviewed and compared to other system logs to ensure:

d. Maintenance tasks continue functioning as expected;

e. Operating systems continue operating within accepted thresholds;

f. System security is not compromised by maintenance tasks; and

g. Maintenance tasks do not adversely affect computer capacity or performance.

Operating System Software Upgrades

Operating system (OS) upgrades shall be carefully planned, executed, and documented as a project. The following steps shall be performed before commencement of an upgrade project:

a. Document that system security controls will remain effective or will be modified to appropriately respond to the OS upgrade;

b. Locate change control processes and procedures;

c. Document agreement of technical staff and management to acceptance criteria;

d. Document that qualified personnel have certified the upgrade and that it has passed user acceptance testing; and

e. Establish a rollback plan in case the upgrade has unacceptable ramifications.

Managing System Operations and System Administration

Systems shall be operated and administered using documented, efficient, and effective procedures to protect State data.

a. The State will establish and maintain an adequate system of controls for IT transaction records, which include access and audit logs related to the activities of IT systems;

b. Controls shall be employed and documented to provide for the management of system operations and system administration. To minimize the risk of corruption to operating systems or integrated applications, the controls include but are not limited to:

c. Develop and document daily operational security procedures;

d. Assigned staff shall perform the updating of the operating systems and program/application backups;

e. Operating system software patches shall be applied only after reasonable testing verifies full functionality;

f. Physical or logical access shall be given to suppliers for support purposes only when necessary and with documented management approval. The suppliers’ activities shall be continuously monitored; and

g. Vendor-supplied software used in operating systems shall be maintained at a level supported by the vendor.

h. Security responsibilities shall be clearly defined for system administrators to protect their assigned information technology resources and information;

i. System administrators shall be appropriately trained; and

j. System administrators shall ensure user access rights and privileges are clearly defined, documented, and reviewed for appropriateness.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

REVISION HISTORY

Revision Date	Summary of Change
01/14/2025	Policy Updates

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK